Appts. and method for re-encrypting data

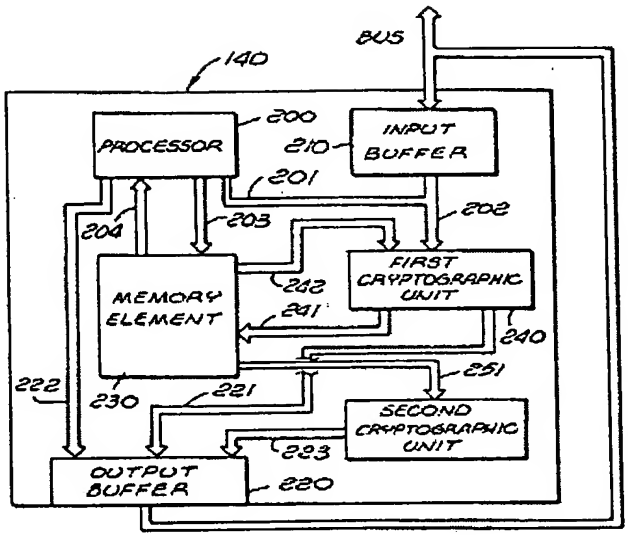
Patent number: CN1222274
Publication date: 1999-07-07
Inventor: DAVIS D L (US)
Applicant: INTEL CORP (US)
Classification:
- International: H04L9/00
- european:
Application number: CN19970195570 19970317
Priority number(s): US19960633581 19960417

Also published as:
WO9739552 (A1)
WO9739552 (A1)
US5805706 (A1)
GB2326571 (A)
BR9708685 (A)

Report a data error here

Abstract not available for CN1222274
Abstract of corresponding document: **US5805706**

A cryptographic device formed as an integrated circuit encapsulated in an integrated circuit package. The cryptographic device decrypts information having a first encrypted format that is input into the cryptographic device producing information in a non-encrypted format. The information in the non-encrypted format is subsequently re-encrypted into a second encrypted format which is output from the cryptographic device. The decryption and re-encryption operations are accomplished entirely within the cryptographic device.



Data supplied from the *esp@cenet* database - Worldwide

[19]中华人民共和国国家知识产权局

[51]Int.Cl[6]
H04L 9/00

[12]发明专利申请公开说明书

[21]申请号 97195570.0

[43]公开日 1999年7月7日

[11]公开号 CN 1222274A

[22]申请日 97.3.17 [21]申请号 97195570.0
[30]优先权
[32]96.4.17 [33]US [31]08/633,581
[86]国际申请 PCT/US97/04697 97.3.17
[87]国际公布 WO97/39552 英 97.10.23
[85]进入国家阶段日期 98.12.16
[71]申请人 英特尔公司
地址 美国加利福尼亚州
[72]发明人 D·L·达维斯

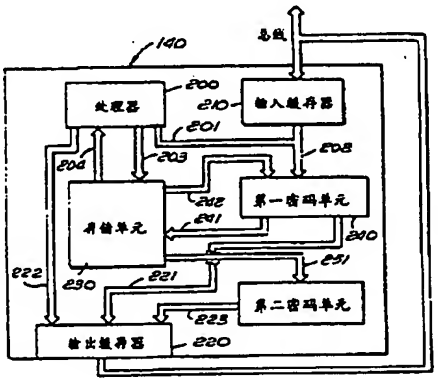
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 邹光新 王忠忠

权利要求书4页 说明书7页 附图页数4页

[54]发明名称 再加密数据的设备和方法

[57]摘要

由封装在集成电路单元中的集成电路构成密码装置(140)。该密码装置(140)将输入到该密码装置的具有第一种加密格式(202)的信息解密成非加密格(241)式的信息。该非加密格式(241)的信息接着再加密成第二种加密格式(223)并从该密码装置(140)中输出。该解密和再加密操作全部都在该密码装置(140)中完成。



ISSN1008-4274

权 利 要 求 书

1. 密码装置接收具有第一种加密格式的输入信息并提供具有第二种加密格式的输出信息，该密码装置包括:

将输入信息解密成非加密格式信息的解密单元；和与该解密单元相连的加密单元，该加密单元将该非加密格式的信息再加密成输出信息，其中，在该密码装置中，将该非加密格式信息从输入信息进行完全解密并再加密成输出信息.

2. 依照权利要求 1 的密码装置，其中该第一种加密格式与第二种加密格式不同.

3. 依照权利要求 1 的密码装置，其中该第一种加密格式与第二种加密格式相同.

4. 依照权利要求 1 的密码装置，其中该解密单元和该加密单元集合为密码处理器，该密码处理器将输入信息解密生成非加密格式的信息并将该非加密格式的信息再加密成输出信息.

5. 依照权利要求 1 的密码装置器件进一步包括在非加密格式信息传输至加密单元之前，对其进行暂时存储的存储单元.

6. 依照权利要求 5 的密码装置，其中该解密单元包括至少一个第一密码处理器和执行存储在该存储单元中的密码算法的处理器.

7. 依照权利要求 6 的密码装置，其中该加密单元包括至少一个第一密码处理器，该处理器和第二密码处理器.

8. 密码装置接收具有第一种加密格式的输入信息并提供具有第二种加密格式的输出信息，该密码装置包括:

将输入信息解密成非加密格式信息的解密装置；将该非加密格式的信息再加密成输出信息的加密装置，其中，在该密码装置中，将该非加密格式信息从输入信息进行完全解密并再加密成输出信息.

9. 密码装置解密具有第一种加密格式的输入信息并生成具有第二种加密格式的输出信息，该密码装置包括:

输入缓存器;

输出缓存器;

与该输入缓存器和该输出缓存器相连的第一密码处理器，该第一密码处理器选择性地将输入信息解密生成非加密格式的信息，并选择性地将该非加密格式的信息再加密成被传送至输出缓存器的输出信

息；

与该输入缓存器和该输出缓存器相连的处理单元，该处理单元选择性地将输入信息解密生成非加密格式的信息，并选择性地将该信息再加密成被传送至输出缓存器的输出信息；

与该第一密码处理器和该处理单元相连的存储器件，至少该信息存储在该存储器件中；

与该存储器件和该输出缓存器相连的第二密码处理器，该第二密码处理器选择性地将该信息再加密成输出信息并将该输出信息传输至输出缓存器。

10. 系统包括：

总线；

与该总线相连的主处理器；

与该总线相连的存储器件；

与该总线相连的密码装置，该密码装置在内部将具有第一种加密格式的输入信息解密成具有第二种加密格式的输出信息，该密码装置包括：

将输入信息解密成非加密格式信息的解密单元；将该非加密格式的信息再加密成输出信息的加密单元，其中，在该密码装置中，将该非加密格式信息从输入信息进行完全解密并再加密成输出信息。

11. 依照权利要求 10 的密码装置，其中该密码装置输入信息的第一种加密格式与输出信息的第二种加密格式不同。

12. 依照权利要求 10 的密码装置，其中该密码装置输入信息的第一种加密格式与输出信息的第二种加密格式相同。

13. 依照权利要求 10 的系统，其中该解密单元和该加密单元集合为密码处理器，该密码处理器将输入信息解密生成非加密格式的信息并将该非加密格式的信息再加密成输出信息。

14. 依照权利要求 10 的系统，其中该密码装置进一步包括在非加密格式信息传输至加密装置之前，对该信息进行暂时存储的存储器件。

15. 依照权利要求 14 的系统，其中该密码装置的解密单元包括至少一个第一密码处理器和执行存储在该存储器件中的密码算法的处理器。

16. 依照权利要求 15 的系统，其中该密码装置的加密单元包括至

少一个第一密码处理器，该处理器和第二密码处理器.

17. 与位于系统远端的远端设备进行通信的系统，该系统包括:

总线;

与该总线相连的存储器件，该存储器件包含数据和指令;

与该总线相连的主处理器，该主处理器执行该指令;

与该总线相连的密码装置，该密码装置在内部将来自远端装置的输入信息进行解密并在内部加密至该远端装置的该输出信息，该密码装置包括:

与该总线相连的第一密码处理器，该第一密码处理器选择性地将输入信息解密生成非加密格式的信息，并选择性地将该非加密格式的信息再加密成输出信息;

与该总线相连的处理单元，该处理单元选择性地将输入信息解密生成输出信息;

与该第一密码处理器和该处理单元相连的存储器件，至少该信息存储在该存储器件中;

与该存储器件和该总线相连的第二密码处理器，该第二密码处理器选择性地将该信息再加密成输出至远端装置的输出信息.

18. 依照权利要求 17 的系统，其中该密码装置进一步包括:

在（i）该总线和（ii）该第一密码处理器和该处理单元间连接的输入缓存器，该输入缓存器接收该输入信息并将该输入信息传输至一个第一密码处理器和处理单元;

在（i）该总线和（ii）该第一密码处理器，该第二密码处理器和该处理单元间连接的输出缓存器，该输出缓存器接收输出信息并将该输出信息放到总线上.

19. 计算机系统包括:

执行指令的主处理装置;

存储该指令的存储装置;

将该主处理装置和该存储装置相连的总线装置;

在内部将具有第一种加密格式的输入信息解密成具有第二种加密格式的输出信息的密码装置，该密码装置包括:

将输入信息解密成非加密格式信息的解密装置;

将该非加密格式的信息再加密成输出信息的加密装置，其中，在

该密码装置中，该非加密格式信息从输入信息进行完全解密并再加密成输出信息。

20. 在内部解密和再加密数据来生成具有所需加密格式的输出数据的方法，该方法包括以下步骤：

接收具有第一种加密格式的数据；

将该数据解密成非加密格式的数据；

将该非加密格式的数据再加密成具有第二种加密格式的数据，其中该解密和再加密步骤全部在该密码装置中完成。

说　明　书

再加密数据的设备和方法

有关申请的相互参考

本申请的发明人已经有两个共同未决的美国发明专利申请，其题目为“提供安全通信的设备和方法”（申请号 08/251，486），“提供安全通信的安全方法”（申请号 08/538，869）和“在硬件代理系统中提供流动软件注册的方法”（申请号 08/472，951）和最近发布的题目为“硬件代理的流动软件注册”（美国专利号 5，473，692）专利．这些申请和专利归本申请的同一受让人所有．

发明背景

1.　发明领域

本发明有关密码学领域．更具体地说，本发明有关将加密信息从一种加密格式编译成另一种格式，而不使其非加密格式暴露的密码装置．

2.　有关本发明的技术描述

在今天的社会中，越来越需要将数字信息（即数据，控制或地址）从一个地点传输到另一个地点，并且该传输方式应该是对于目标用户来说是清晰和明了的，而对于任何非法侵入者（illegitimate. interloper）则是不可理解的．因此，在传输前，该数字信息通常被主处理器通过储存在主存储器中的加密算法进行加密．对于该加密使用了该目标用户所特有的通信密钥．此后，该目标用户为了他或她的使用而将该加密信息解密．这种传统的密码传输技术通常使用在政府的应用中，同时也使用在对于传输敏感信息（例如机密的，涉及所有权的信息等）的商业应用中．

而且，进一步地，最好是将数字信息以加密格式存储在与计算机相关的主存储器或大容量存储装置中．这样做可以避免非法者从主存储器或大容量存储装置中，下载非加密格式（即普通文本（plain text））的敏感信息至软盘中．然而，不管是以加密格式存储信息，还是传统的密码传输技术，都不能充分地避免普通文本的不安全的暴露（即在执行密码算法的器件的范围之外）．例如，为了将加密文件从一个计算机传递到另一个计算机，该加密文件将被解密成普通文本，然

后用指定给目标接收者的通信密钥进行再加密．这样，该普通文本将至少暴露在系统总线上，当文件的大小大于主存储器的容量时，该普通文本将暂时存储在计算机的大容量存储装置中（例如内部硬盘）．这种暴露的问题给有关的安全方面带来了一些缺点．

一个明显的缺点是，当普通文本没有从内部硬盘上及时清除或者其它计算机可以通过局域网读取该硬盘时，该普通文本文件可以被非法者读取．即使是发送者经常从硬盘上清除该普通文本或者该普通文本文件从不存储在硬盘上，也存在着侵入者通过软件（例如计算机病毒）或硬件装置（例如逻辑分析器）来简单地监视计算机的系统总线，以获取该普通文本的可能性．

另一个缺点是，当信息要以加密格式送至负责用不同的加密格式对信息进行再加密的第三方（例如系统管理员）时，没有机制来保证只有确定的接收者能读取所包含的信息．

还有另一个缺点是，没有机制来保证避免由内容分配或者软件包所提供的数据的非法使用（即拷贝保护）．

因此，最好能够生成一种密码装置（crytographic device），该密码装置能够充分地减少访问非加密格式信息（即普通文本）的可能性，该信息最初以一种加密格式存储在一种信息源中，并且需要以另一种或甚至相同的加密格式转换到另一种信息源中．该密码装置将最终消除任何侵入者盗取安全信息的可能性，因为侵入者必须通过芯片内的集成电路来获得该信息，这显然比通过总线来获得信息要难得多．

发明摘要

本发明有关密码装置，该密码装置将输入到密码装置中的具有第一种加密格式的信息解密生成非加密格式的信息．该非加密格式的信息接着用第二种加密格式再加密．该具有第二种加密格式的信息从该密码装置输出．该加密和再加密操作全部在密码装置内部完成．

附图简述

本发明的特征和优点将通过下面本发明的详细描述阐述得更加明了．其中：

图 1 为包含与本发明相关的密码装置的计算机系统框图．

图 2A－2D 为密码装置的各种实施例的描述性框图．

图 3 为密码装置的另一种描述性实施例的更加详细的框图．

图 4 为描述防止在密码装置之外获得普通文本信息的方法的流程图.

发明详述

本发明涉及将信息从一种加密格式译成相同的或另一种加密格式的信息，而不使该中间的普通文本暴露在不安全环境下的设备和方法. 在下面的描述中，列举了大量的细节以使对本发明有透彻的理解. 然而，显然对于那些本领域的技术人员来说，本发明可以通过很多与所描述的不同的实施例来实现，而并不偏离本发明的精神和范围. 另外，为了避免给本发明带来不必要的晦涩，没有详细地列出众所周知的电路，器件等等.

在详细的描述中，频繁地使用了一些与密码学相关的词来描述一些本文所描述的特征或特点. “通信密钥”是密码算法所使用的编码和/或解码参数，该密码算法例如为使用公用和私人密钥对的 Rivest, Shamir, 和 Adleman (“RSA”) 算法和使用两对间秘密共享的选择密钥的数据加密标准 (“DES”) 算法. 通常，该通信密钥是“n”比特长的二进制数据的连续分布 (“串”)，其中“n”为任意数. “文件”通常被定义为在一序列总线周期中传输的信息 (例如数据，地址，密钥等). “普通文本”定义为非加密格式的信息，它包括但不限于表示文本的数字数据，视频音频和其它媒体数据.

参照图 1，描述了利用本发明的计算机系统 100 的描述性实施例. 该计算机系统 100 包括一系列子系统，该子系统包括处理器子系统 110，存储器子系统 120 和输入/输出 (“I/O”) 子系统 130. 这些子系统和密码装置 140 通过系统总线 150 连接在一起，使得信息可以在子系统和密码装置 140 间进行通信. 可以考虑将该密码装置 140 改变为与 I/O 总线 160 相连 (例如 PCI 总线或 ISA 总线)，与主处理器 111 中的局部总线或任何总线机制相连.

该处理器子系统 110 包括执行来自存储器子系统 120 的指令和处理来自计算机系统 100 的信息的主处理器 111. 尽管只画出了一个主处理器 111，可以考虑在计算机系统 100 中应用不止一个处理器. 而且，该存储器子系统 120 可以包括存储控制器 121，该存储控制器控制对一个或多个存储器装置 122 的存取，例如动态随机存取存储器 (“DRAM”)，只读存储器 (“ROM”)，视频随机存取存储器 (“VRAM”) 等等. 该存储

器装置 122 存储主处理器 111 所使用的信息.

该 I/O 子系统 130 包括作为 I/O 总线 160 和系统总线 150 间接口的 I/O 控制器 131. 这提供了连接到不同总线的设备间信息交换的通信路径. 该 I/O 总线 160 至少对一个计算机系统 100 中的外围设备输入或输出信息. 举例来说, 该外围设备可以包括但不局限于显示装置 132 (例如阴极射线管, 液晶显示器, 平面显示器等等); 字母数字输入装置 133 (例如密钥盘, 密钥板等); 光标控制装置 134 (例如鼠标, 轨迹球, 触摸板, 游戏杆等); 大容量数据存储装置 135 (例如磁带, 硬盘驱动器, 软盘驱动器等); 将信息从计算机系统 100 传输至远端系统或从远端系统传回的信息收发装置 136 (传真机, 调制解调器, 扫描仪等); 和硬拷贝装置 137 (例如绘图仪, 打印机等). 可以考虑如图 1 所示的计算机系统使用这些器件的部分或全部, 或者使用与所画出的器件不同的器件.

在计算机系统之外, 可以进一步考虑在任何依靠加密通信的电子系统中加入密码装置 140. 例如, 这些电子系统可以包括有线电视控制盒, 银行自动柜员机 ATM 和接收一种加密格式的信息并以另一种加密格式发送或存储该信息的网络外围节点. 这些例子是说明性的, 不应理解为本发明的限制.

现参照图 2A, 该密码装置 140 与系统总线相连, 允许其由信息收发装置接收具有选择加密格式的信息 (例如文档, 文件) 并将该信息再加密 (即接着加密) 为另一种加密格式. 该密码装置 140 包括一个或多个封装在集成电路器件单元 142 中的集成电路 141, 最好是密闭封装, 以避免该集成电路 141 受到损伤, 有害污垢的影响并使侵入者更加难以获得普通文本或关密钥信息. 该集成电路 141 具有与加密单元 144 相连的解密单元 143, 在 Bruce Schneider 所写的, 1996 出版的, 题目为 "应用密码学第二版: 协议, 算法和 C 源代码" 的出版物中描述了这两个单元的功能.

该解密单元 143 接收第一种加密格式 ("加密数据入") 的信息并解密该信息. 这样, 该解密单元 143 配置了必要的通信密钥 "密钥$_{入}$" 来解密信息, 生成普通文本信息. 此后, 该解密单元 143 可以通过硬件来实现相应的功能. 该加密单元 144 接受普通文本并依照所选择的通信密钥 "密钥$_{入}$" 来再加密生成再加密信息 ("加密数据出"). 该加

密信息从密码装置 140 输出至存储器子系统或用来存储的大容量存储装置，或输出至用来传输至远端系统的收发单元.

该解密单元 143 和加密单元 144 可以通过硬件来实现上述的功能. 显然，该解密单元 143 和加密单元 144 可以是执行密码算法和在安全环境中维护普通文本的一般意义上的微处理器，或者是任何能够实现这种解密或加密功能的智能电子装置.

可以考虑使用其它实现方式. 例如，在图 2B 中，可以在解密单元 143 和加密单元 144 中插入缓存器 145 来暂时存储普通文本. 如果加密格式的差别需要进行时间调整，那么该方案就是必要的. 在图 2C 中，解密和再加密是由同一密码“单元”146 处理的，该密码单元最好是从缓存器 147 回送普通文本，来在输入信息的解密之后进行再加密. 在图 2D 中，解密和再加密是通过从存储器器件 149 中获得必要的加密和解密算法的处理器 148 来实现的. 输入至密码装置 140 的加密数据和从密码装置 140 输出的加密数据都通过经过与图 2A-2C 相似的不同的连接管脚的总线来传输.

参照图 3，结合在图 2A-2D 中显示的特性，显示了一般意义的密码装置的更加具体的框图. 该密码装置 140 包括处理器 200，一些缓存器 210 和 220，存储器件 230 和一些密码单元 240 和 250. 该密码装置 140 接收加密输入信息，该加密输入信息一般来自与 I/O 总线相连的装置，例如大容量存储装置或信息收发装置，或来自主处理器. 根据输入信息的加密格式，该加密信息可以选择性地通过通信线 201 传输至处理器 200 或通过通信线 202 传输至第一密码单元 240. 该路由选择通常由主处理器 111 来实现. 控制信息流动的原因是由于每个密码单元只能解密一种加密格式的信息，而处理器 200 可以设置为以较慢的速度执行在存储器件 230 中的密码算法来实现加密或解密.

在加密信息传输至第一密码单元 240 时，该第一密码单元 240 将该加密信息解密成普通文本并通过通信线 241 将该解密信息传输至存储器单元 230 中. 另外，在加密信息传输至处理器 200 时，该处理器 200 执行特殊的密码算法来将该加密信息解密并通过通信线 203 将普通文本形式的解密信息传输至存储器单元 230 中.

为了将该普通文本加密成第二种格式，可以依照三种可替代的数据路径. 第一种数据路径是在该处用所接收信息的相同格式来加密普

通文本．这样，该普通文本通过通信线 242 传输至第一密码单元 240，这时，该密码单元 240 将普通文本解密为第一种密码格式并通过通信线 221 将该信息输出至输出缓存器 220 中．第二种数据路径是在该处需要用第一和第二密码单元 240 和 250 所提供的以外的加密格式对普通文本进行加密．在这种情况下，该普通文本通过通信线 204 传输至处理器 200．该处理器 200 接收普通文本并通过执行一种相关的密码算法加密该信息．此后，该处理器 200 通过通信线 222 将该加密信息传输至输出缓存器 220．第三种可替代的数据路径是在该处用第二密码单元 250 所提供的格式对普通文本进行加密．该普通文本通过通信线 251 提供给第二密码单元 250．该第二密码单元 250 将普通文本加密成第二种加密格式并通过通信线 223 将该信息传输至输出缓存器 220．此后，该输出缓存器 220 将该加密信息传输至系统总线中，用来在存储装置或大容量存储装置中存储该信息，或通过信息收发装置传输至远端系统．

可以考虑通过只是加密至少一部分文件分配数据来进行拷贝保护，该数据将被解密，处理和加密，以便在密码装置中存储．

现参照图 4，显示了描述对输入至密码装置中的数据进行再加密操作的流程图．在步骤 300 中，以第一种格式进行加密的数据输入至该密码设备中．接着，在可选步骤 305 中，该加密数据由于时间的关系被缓存．接着，在步骤 310 中，该加密数据利用所描述的密码算法和通信密钥进行解密．该操作可以选择实现方式，通过硬件或软件来实现．在解密数据时，如果需要（步骤 315），该普通文本可以存储在随机存取存储器（在装置 140 中）中．此后，在步骤 320 中，当需要加密格式与输入到密码装置的格式不同时，该普通文本利用第二种描述的密码算法和通信密钥进行加密，而当在加密包括与输入端接收的格式相同格式时，就使用第一种指定的密码算法和通信密钥进行加密．然后，在可选步骤 325 中，与步骤 305 相似，该加密数据由于时间的关系被缓存．此后，该再加密数据从密码装置输出，来存储在大容量存储装置中或通过信息收发装置 330 进行传输．

在这里所描述的本发明可以用很多不同的方法和使用很多不同的设置来设计．尽管用各种实施例对本发明进行了描述，对于那些本领域的技术人员来说，可以想到并不偏离本发明的精神和范围的其它的

实施例。因此，本发明应通过下面的权利要求来衡量。

说 明 书 附 图

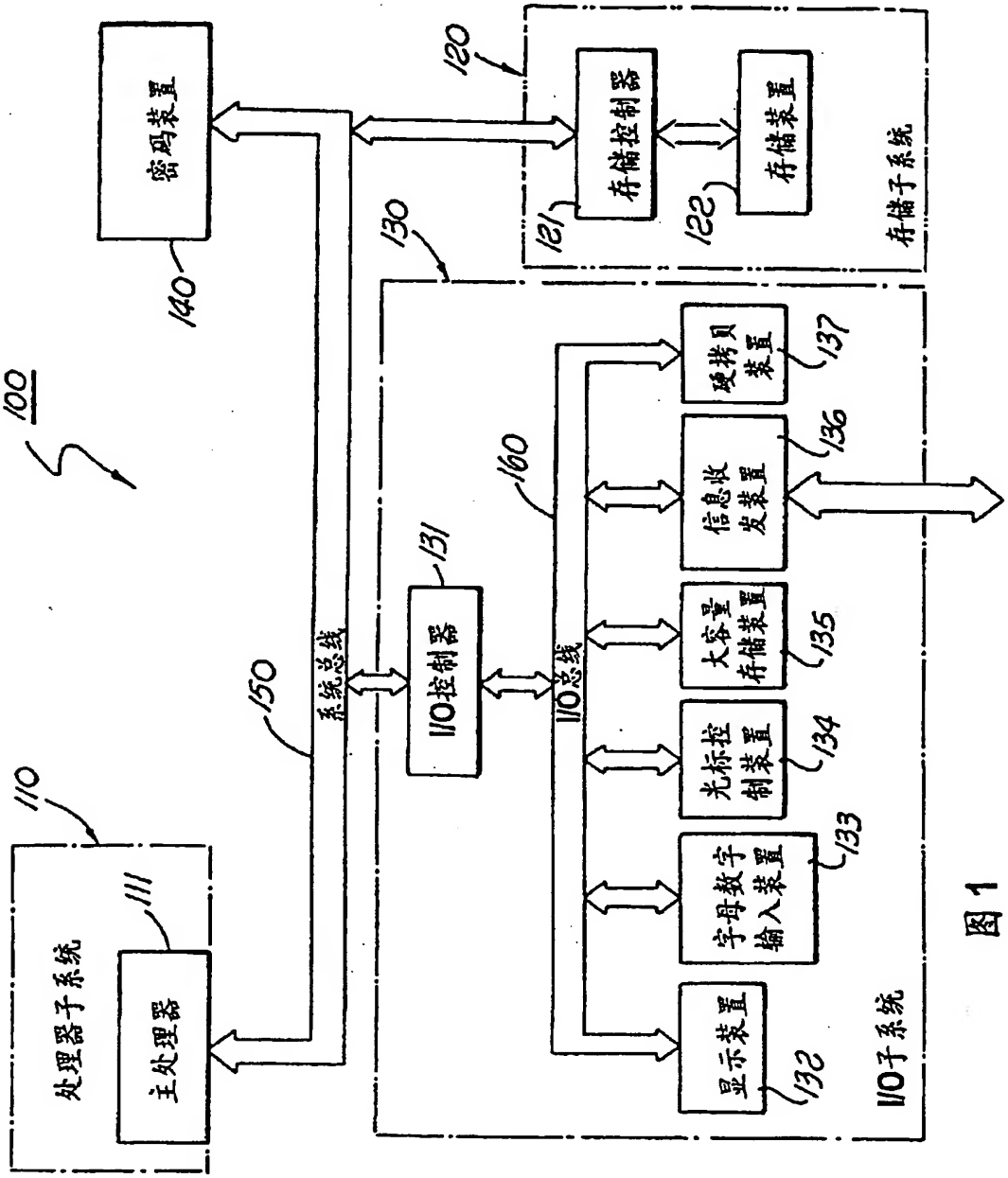

100
处理器子系统
110
主处理器
111
密码装置
140
系统总线
150
120
存储控制器
121
存储装置
122
存储子系统
130
I/O控制器
131
I/O总线
160
硬拷贝装置
137
信息收发装置
136
大容量存储装置
135
光标控制装置
134
字母数字输入装置
133
显示装置
132
I/O子系统

图 1

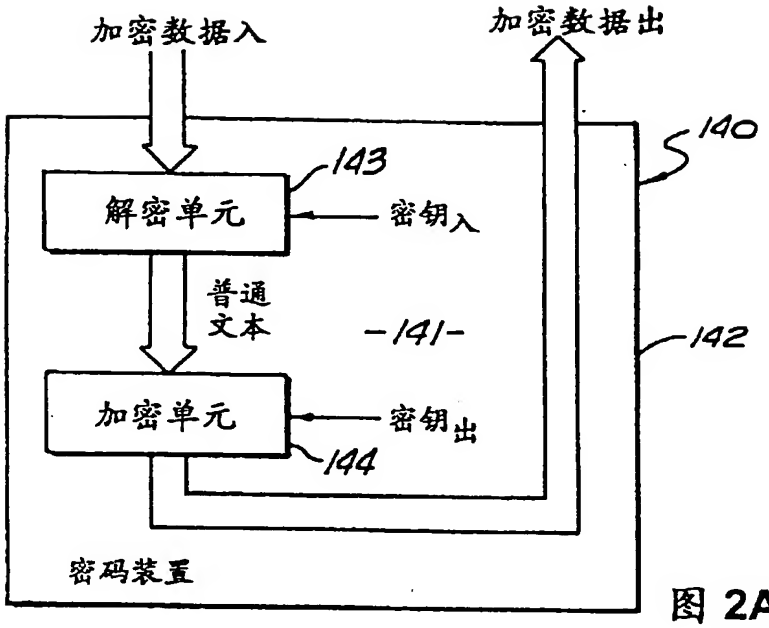

加密数据入
加密数据出
140
143
解密单元
密钥入
普通
文本
141
142
加密单元
密钥出
144
密码装置

图 2A

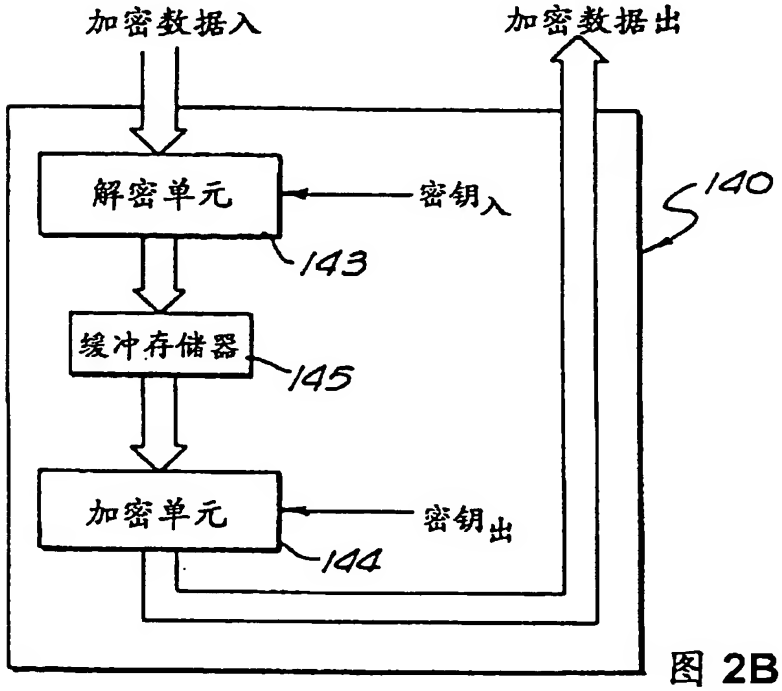

加密数据入
加密数据出
140
解密单元
密钥入
143
缓冲存储器
145
加密单元
密钥出
144

图 2B

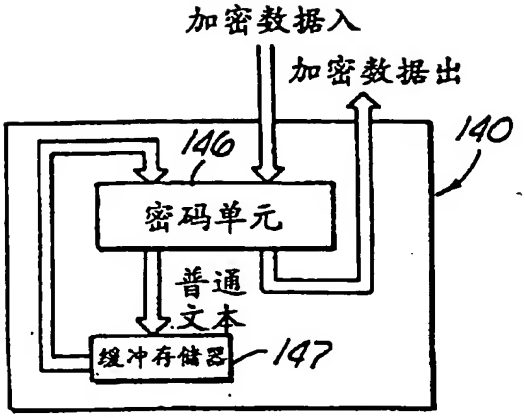

加密数据入
加密数据出
140
146
密码单元
普通
文本
缓冲存储器
147

图 2C

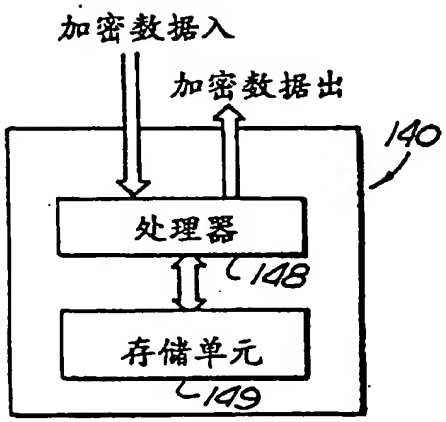

加密数据入
加密数据出
140
处理器
148
存储单元
149

图 2D

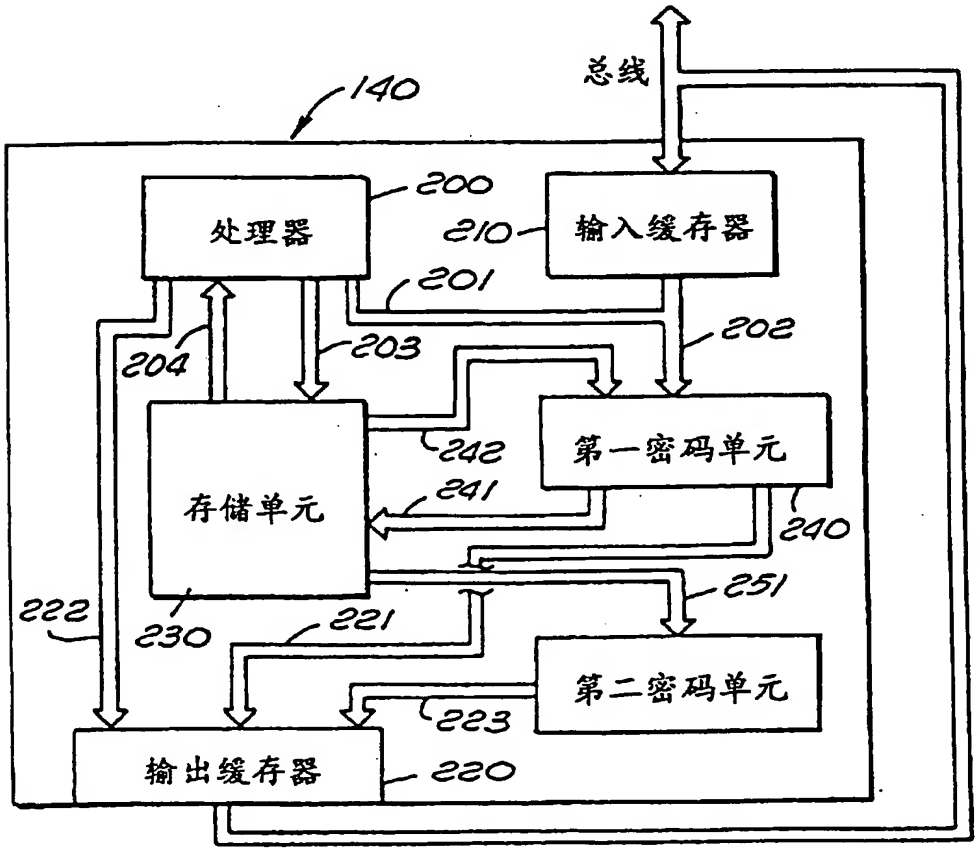

140
总线
处理器
200
210
输入缓存器
201
202
203
204
存储单元
242
第一密码单元
241
240
251
222
230
221
第二密码单元
223
输出缓存器
220

图 3

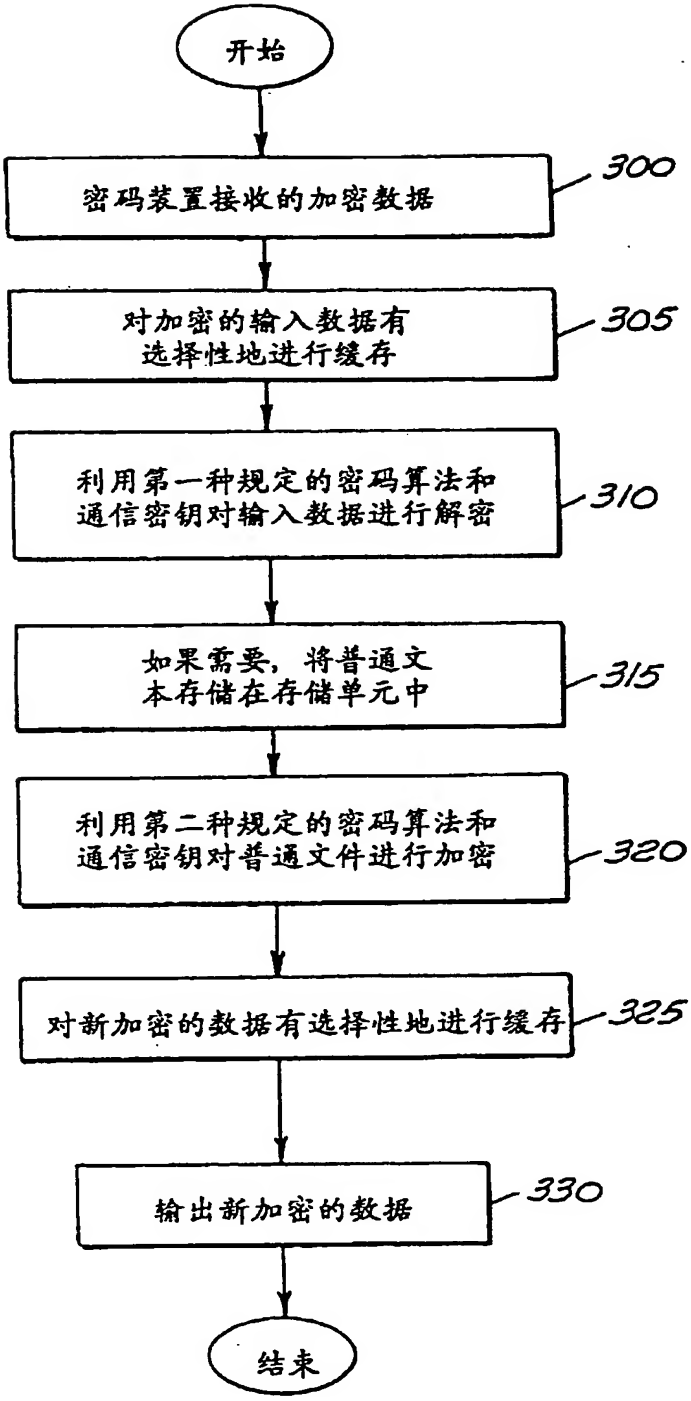

开始
密码装置接收的加密数据
300
对加密的输入数据有选择性地进行缓存
305
利用第一种规定的密码算法和通信密钥对输入数据进行解密
310
如果需要，将普通文本存储在存储单元中
315
利用第二种规定的密码算法和通信密钥对普通文件进行加密
320
对新加密的数据有选择性地进行缓存
325
输出新加密的数据
330
结束

图 4